The Need for Information Sharing and Analysis Organizations to Combat Attacks on States and Communities

Gregory White Ph.D.
UTSA CIAS
Greg.White@utsa.edu

Keith Harrison Ph.D.
UTSA CIAS
Keith.Harrison@utsa.edu

Natalie Sjelin
UTSA CIAS
Natalie.Sjelin@utsa.edu

Abstract

An ever increasing number of attacks are being reported on various city and state computer systems and networks worldwide. These attacks have resulted in the disruption of city operations or the release of personal information. Cities and states need to protect their systems but frequently plans to do so are lacking and the ability to respond to cybersecurity events is non-existent. This is especially true for smaller communities that do not have the budget to hire full-time security personnel or contract for security services. A critical step that states and communities can take is the establishment of a state or community Information Sharing and Analysis Organization (ISAO). This paper will describe how a state or community can use the creation of an ISAO to jumpstart various aspects of its cybersecurity program, incorporating a number of established programs in a single initiative.

1. Introduction

Protection of a nation's cyber infrastructures is now generally accepted to be critical to the nation's security and survival. Most nations have focused their efforts on securing the various critical infrastructures as well as government agencies and organizations. This is true in the United States where the Department of Homeland Security has spent considerable time and resources on securing the nation from a higher-level, or national level. This has left states and communities to often "fend for themselves". At the same time, for a variety of reasons, states and communities have been increasing their efforts to provide citizens access to various government services. This has led to numerous attacks that communities have experienced on their computer infrastructures. Reports in the media have attested to this and local officials have recognized the growing risk to their communities. In September 2017, *Government Technology* stated that:

> *Nearly 40 percent of local government CIOs report experiencing more attacks during the last 12 months, according to a 2016 survey by the International City/County Management Association (ICMA). And the frequency is increasing too, with 26 percent of CIOs reporting an attack, incident or breach attempt occurring hourly, while another 18 percent report a cyber attempt at least daily.*
>
> *That's bad news for local governments, which have fewer resources than many larger jurisdictions to fight back. But it's especially bad for small to mid-sized cities, counties and towns, which may have only one full-time person devoted to IT — including cybersecurity — if they are lucky.* [1]

There are three important points highlighted in this statement: 1) Communities have been the target of cyber attacks; 2) The rate of attacks is increasing; and 3) Communities have limited resources to address the cybersecurity challenge.

There are various models and frameworks that have been developed to address the creation of cybersecurity programs within organizations – including communities. Similar to the point made in the quotation from *Government Technology*, small to mid-sized cities, counties, and towns who have very limited resources to devote to cybersecurity also generally don't know how to establish a viable cybersecurity program and how to utilize the models and frameworks available to them. There have been limited attempts to explain how all of these can come together to help secure a community but the recent emphasis on the value of information sharing over the last few years provides an opportunity to provide the needed impetus and roadmap for communities to establish and mature their cybersecurity programs. In particular, this paper will focus on three elements: 1)

URI: https://hdl.handle.net/10125/59722
ISBN: 978-0-9981331-2-6
(CC BY-NC-ND 4.0)

Establishment of a community Information Sharing and Analysis Organization (ISAO) and understanding the benefit of sharing across the different sectors in a community; 2) Implementation of the Community Cyber Security Maturity Model (CCSMM); and 3) Use of the NIST Cyber Security Framework at the appropriate point in the development of the community's security program.

2. Information Sharing

The start of formal information sharing for cybersecurity purposes within the United States began in 1998 with the publication of the Presidential Decision Directive NSC/63 (PDD 63).[2] This directive from the White House, signed by President Clinton, was aimed at measures to better protect the critical infrastructures for the nation. One of the proposed efforts was to form Information Sharing and Analysis Centers (ISACs) for each of the critical infrastructures identified by the government. These centers were to share "important information about vulnerabilities, threats, intrusions and anomalies" within each of the sectors and to provide this information to the federal government as well. The federal government was also supposed to share information pertinent to the various critical infrastructures with each of the ISACs.

One of the initial concerns expressed by members of the various critical infrastructures, and by skeptics of the program in general, was why would organizations share information with potential competitors that might be used against them in a competitive environment? This has been overcome within the sectors as organizations have come to realize the benefit of sharing information. To illustrate the point, the financial services sector has one of the most robust and capable ISACs today. The Financial Services ISAC (FS-ISAC) has thousands of members both within the United States and abroad. If one of its members, Bank Alpha, discovers an intrusion or an attack on their systems and network, there is a probability that others within the banking community might also be experiencing the same attacks. Bank Beta may not have detected the attacks but if Bank Alpha shares that information with the FS-ISAC who then passes it on to all of its members, Bank Beta would be warned and would be able to determine that they too were under attack. This time it was Bank Alpha that noticed the attack first. The next time it might be Bank Beta that first notices the indications of an attack. Collectively, the banks realize that they are better off sharing information with each other. This scenario applies to organizations within any sector.

It is important to note that in effect, the financial services community (and others) have learned that while the ISAC consists of a number of financial institutions that are in competition with each other, when it comes to cybersecurity, the banks are not competing against each other, but are competing against the cyber attackers. From the community perspective, the financial services organizations work together to compete against adversaries attacking its members and are not in a battle between the members themselves.

Cybersecurity information sharing took another step forward in 2015 when President Obama issued Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing. [3] This document extended the information sharing ecosystem beyond the critical infrastructures to create Information Sharing and Analysis Organizations (ISAOs) which would include any "sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities." [3] This executive order was a result of the realization that the majority of the nation did not fall into one of the critical infrastructures but would still benefit from being part of an information sharing program.

One important point in the executive order was the recognition that an ISAO could be based on a geographic region. This has led to the development of a few state ISAOs and discussions about community ISAOs. An ISAO based on a region would potentially include members from many different sectors – both critical infrastructures as well as sectors not considered critical. The benefit of such an organization was seen in research conducted in support of efforts to define processes for community incident detection and response. Specifically, in work which led to the development of a "Honey Community." [4]

2.1. The Honey Community

The Honey Community was created to provide useful data on attacks that occur on a community. Instead of monitoring the networks of a real community, the researchers created a fake community and provided a website for it. The website included various sectors that are typically found in a community including such things as public utilities, local government offices, and a school district. Similar to other honey devices, it was created and then monitored for a short period of time.

The data was then used to examine possible ways to detect an attack that was occurring on a community.

What was notable about the data gathered was discovered when looking not at any one of the individual sectors but across the sectors. In the short period of time the Honey Community was available, there were 3060 identified attacks. These occurred on one or more sectors. Of the 3060 attacks, 1430 were identified as an attack on a single sector, 151 on 2 sectors, 52 on 3 sectors, 16 on 4 sectors, and 9 on all 5 sectors. [4] This was interesting data but the researchers were surprised when they examined the data and realized that 1402 attacks would not have been identified by looking at any one of the sectors individually. These were noticed as attacks only when examined across the community. This was a significant finding because in almost all cases, individual sectors in a community (or state) confine their discussions on security events to others in the same sector or to individuals that may not be in the same sector but are known personally. If the community wants to have the best chance at detecting intrusions information needs to be shared across all sectors within the community.

2.2. The Multi-State ISAC

The mission of the Multi-State ISAC (MS-ISAC) is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery. Some may already know about its existence and believe that it is designed to provide the information sharing needed by a community. While the MS-ISAC has a very large number of members from states and communities around the nation, it is not sufficient for all that is needed in a community. It is an important element, and communities should be members of the MS-ISAC, but there is a side of information sharing that relies on trust which is often hard to obtain in an organization as large as the MS-ISAC. While members trust the MS-ISAC, they may not be comfortable with other members of the organization and indeed will not know all of the members of the group. Trust can be more easily obtained through personal contact and working with individuals which a community ISAO will more easily be able to provide.

3. A Community Maturity Model

A problem that states and communities frequently face is not knowing where to begin in establishing their cybersecurity programs. Many community leaders are unaware of the significance and importance of such a program, but even when made aware, how to get started on one is a daunting process. One effort at making states and communities aware of the cybersecurity challenges they faced started in 2002 with the first community cybersecurity exercise. Following this first exercise, which took place in San Antonio, TX, a number of other state and community exercises were conducted. These were extremely successful in making local leadership aware of the type of issues that they faced. What they didn't do, however, and what was not realized until the communities were visited again, was the communities did not have a mechanism or plan to move the community forward. What should they do first in establishing a viable cybersecurity program? What needs to be done next? What can be postponed until the program is more mature? There were plenty of vendors willing to supply services or products but how does the community decide what is really needed at the start and what can be purchased at a later date? The monetary concerns were especially problematic as almost no community had a budget already established for implementing a cybersecurity program.

The researchers conducting the exercises took a step back at that point and developed a plan via the creation of the Community Cyber Security Maturity Model (CCSMM). [4] This model provided three things: 1) It served as a 'yardstick' so that a state or community could measure where it was in terms of its security program; 2) It provided a roadmap for what a state or community needed to do in order to move from one level in the model to the next; and 3) It provided a common point of reference so that two communities could discuss their programs with each other and have an understanding of what each is trying to achieve.

The model addresses specific areas a community needs to improve when it comes to cyber threats. The areas of improvement are called *dimensions*. There are four dimensions identified in the CCSMM. They are **awareness, information sharing, policies** and **planning**. Each of these dimensions has five levels of maturity. The levels begin at the **Initial** level (Level 1), which is where every community begins, and builds a roadmap for communities to improve to reach the **Vanguard** level (Level 5). Level 5 is the stage where cybersecurity is a business imperative and is simply incorporated into every aspect of government, industry, and public life.

The improvements are accomplished with *implementation mechanisms*. The implementation mechanisms allow a community to progress from one level to the next in each dimension. The implementation mechanisms are the activities used to:

- Increase awareness
- Establish information sharing practices
- Add cyber components to policies in a meaningful way
- Incorporate aspects of cyber security into continuity plans

The implementation mechanisms are:

- Metrics
- Processes and procedures
- Technology
- Training
- Assessments

A community can progress at its own pace along the lines of any of the dimensions as it progresses from one level to the next. Training at each level of each dimension helps to provide the necessary information for the community to advance. Technology may also be needed and policies should establish the goal at each level for each dimension. Taken together, these element help the community to plan for the progression of its program as it first establishes a viable program and then increases the ability to address cybersecurity events.

After development of this model, the researchers proceeded to provide information on the model and how to use it to additional states and communities around the nation. It was well received and feedback from individuals indicated that it was easy to understand and follow.

The model did a lot to help provide an organized approach to cybersecurity at the state and local level. It was adopted by the National Cybersecurity Preparedness Consortium (NCPC) to organize the efforts of its members around it. The NCPC is a five-university consortium dedicated to providing "research-based cybersecurity-related training, exercises, and technical assistance to local jurisdictions, counties, states, and the private sector. [5] The consortium has provided on-line and classroom-based training to every state and territory in the U.S. and continues to develop training courses to fill the gaps in the CCSMM where no training currently exists.

While the model has been a useful aid to states, territories, and communities it has not proven to be the catalyst that is needed to energize communities around the nation. In communities where there is a strong champion for cybersecurity who is in a position of authority, the model can serve the purpose it was designed for and the community can move forward in an organized manner to implement a viable and sustainable cybersecurity program. If there is no champion, however, cybersecurity efforts tend to languish and there will be a momentary surge in interest which then gradually gets lost in the day-to-day operational issues facing a city. Unless the city is hit with a cybersecurity event of some sort, such as ransomware or a security breach of an important system, the community is likely to continue with only minor efforts to secure their critical cyber infrastructures. What is needed is a catalyst that will inspire all communities to develop their cybersecurity programs and that provides some guidance on what needs to be accomplished. The National Institute of Standards and Technology (NIST) developed a framework with the hope that it would provide the guidance that not only federal departments and critical infrastructures could follow but that could also be utilized by industry and the nation in general. This framework is called the Cyber Security Framework (CSF).

4. The Cyber Security Framework

NIST published version 1.1 of what is commonly referred to as the Cyber Security Framework in April 2018. The official title, "Framework for Improving Critical Infrastructure Cybersecurity", better describes the original focus of the document. While the original intent was to address the security of the critical infrastructures, the document is valuable for organizations in any sector. As described in the Executive Summary for the framework:

> *While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.*
>
> *The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for*

cybersecurity, the Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities. [6]

At the heart of the framework is a set of activities that should be considered as part of every cybersecurity program. These issues are:

1) Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
2) Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
3) Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4) Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
5) Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. [6]

These five elements are referred to as *Functions* in the framework. They are used to organize specific cybersecurity activities at the highest level. These many different cybersecurity activities are further organized into *Categories* of activities with similar outcomes that fit into each Function. The Categories are further subdivided into *Subcategories* of "specific outcomes of technical and/or management activities." Finally, the items found in the various Subcategories are provided references to the standards, guidelines, and practices that illustrate ways that the desired outcomes can be achieved. When taken in its totality, the framework points organizations to a vast amount of knowledge on cybersecurity issues.

The CSF provides a tremendous amount of useful information and for large organizations, whether in government or industry, it is a valuable tool or guide that can be used to address the key cybersecurity issues of identification, prevention, detection, response, and recovery. The key, however, is to be able to fully utilize the CSF and to use it as guidance on what your cybersecurity program needs to include can be a daunting task often requiring individuals with a firm grasp on cybersecurity. Simply handing the CSF to an IT professional in a state or community or to a small- or medium-sized business could easily lead to frustration due to the sheer volume of information contained in it. What is needed is step-by-step guidance to assist individuals in how to incorporate the information referenced and described in the CSF into their own cybersecurity program. NIST has provided additional guidance on how to implement the framework but incorporating the efforts into the other programs mentioned will better help to guide states and communities on how to ensure they address each activity at the appropriate point in the development of their individual programs.

5. The Elements of a Combined Approach

None of the initiatives described so far have proven to be the panacea states and communities require to develop and sustain their cybersecurity programs. Each, for different reasons, are not individually sufficient to provide the needed guidance that will help to put a state or community on the path to develop a sustained cybersecurity program. If, however, the programs are combined in a coordinated fashion, the three requirements needed for developing a program can be realized. Specifically, what is needed (and which is provided by each) is:

1) A champion or organization that will ensure that the program does not get dropped as interest inevitably wanes and other priorities emerge. With the nature of an ISAO and with the current impetus to increase the level of information sharing, an ISAO can help ensure the program does not languish and devolve into an ineffective organization.
2) A framework that describes the areas the program needs to include and that provides guidance for where to find more detailed

information about each aspect of the security program. The CSF does an excellent job in providing this information.

3) A roadmap for what needs to be done first and what can be implemented at a later time. The CCSMM was designed for this purpose and by including the other two elements into the model it can provide a step-by-step approach for a state or community to develop its sustainable cybersecurity program. Keep in mind it is likely the case that as the process begins, there will not be a budget to accomplish this and the steps need to begin with items that are at no or low cost.

Currently there are a lot of discussions about the benefits of sharing cybersecurity information. With legislation such as the Cybersecurity Information Sharing Act of 2015 and with an increased concern about the security of our critical infrastructures, sharing of information about security vulnerabilities and incidents has become a hot topic. Sharing of information, however, is not the total solution – organizations have to know what to do with the information they receive and how best to adapt to the ever-changing security environment. An ISAO by itself is insufficient for the establishment of the viable security program discussed. With the interest in it and support from organizations such as the Department of Homeland Security, it is a great entity from which to build the other parts of a state or community security program.

6. Creating a Community ISAO

The first step in the coordinated approach to cybersecurity within a community or state will be the establishment of the community or state ISAO. An important aspect of these ISAOs is the cross sector nature of the organization. The ISAO will serve to encourage discussions of security topics across the state or community. An important point to remember for ISAOs is that they need to be sharing more than just information about vulnerabilities and indicators of possible intrusive activity. These are both important but the design of the new breed of ISAOs is the encouragement of sharing other information such as best-practices, training, and assessment of security technology. The ISAO will assist the state or community in staying engaged in cybersecurity awareness, information sharing practices, cybersecurity processes and overall plans to integrate cybersecurity into their community's continuity of operations. Essentially, the State or community ISAO will become the cybersecurity champion for the state or community. More specifically, an ISAO can assist with the following:

- Workshops, seminars, webinars and in-person meetings
- Providing or sharing training on security awareness, security tools and capabilities
- Developing cybersecurity strategies including no- and low-cost initiatives addressing cybersecurity
- Developing processes connecting local governments with small businesses in their jurisdictions
- Discussing implementation of DHS cybersecurity initiatives available to the States and Local governments
- Creating public private partnerships within a geographic area

In addition, a state ISAO can serve to bring the communities within the state together to cooperatively work together on their security programs. Some communities will naturally progress faster than others in the establishment of their programs and the state can help bring more mature communities together with those just starting on their programs to assist in the state's overall security status. We have seen in the past several years that smaller communities are often the target of attackers and a mentor from another community could greatly assist in learning what works in the creation of a community security program.

In establishing an ISAO, a critical step is to define the mission and goals of the Community ISAO (a similar step should be taken for a state ISAO). Having specific goals and a mission statement will help to drive the structure needed to accomplish the goals and provide guidance on which organizations (or members) should participate in the ISAO. It is important to note that inclusion in a state or community ISAO by an organization does not preclude participation in other sector-based ISAOs as well. For example, a local community bank could be part of the Financial Services-ISAC and also part of the community ISAO in which they reside. The benefit of being in both is that they will receive sector-based information from the FS-ISAC but will find out about what is going on in the community from their community ISAO. Remember the research mentioned earlier that showed that almost half of the attacks that occurred in a community would have gone undetected if the information was not shared between sectors. A community ISAO also has the benefit of physically bringing members closer

together since having an in-person meeting or workshop is a lot easier in a community as opposed to a national sector-based ISAC. This personal aspect lends to the development of a level of trust between members and greatly facilitates the sharing of information. A final consideration for a community ISAO is in defining who the members will be. Will the ISAO extend its services to organizations within the city limits, or will counties also be included and how far out geographically will the ISAO extend?

Once we have established our goals and defined the potential members, we will need to implement programs and training that will encompass the varying states of cybersecurity preparedness our potential organizations may be at. This is where the CCSMM will become a key asset as it will guide the development of needed programs that will improve each organization's cybersecurity posture in awareness, information sharing, processes and planning. Essentially, the CCSMM will be the mechanism the ISAO will use to develop programs that will assess what level of capability an organization is at and will provide the roadmap needed to improve the organization's overall cybersecurity. Enhancing each organization's cybersecurity posture will improve the overall community cybersecurity preparedness.

It should be noted that as an ISAO starts working on implementing the CCSMM within the state or community, it is actually extending itself beyond what has traditionally been defined as an Information Sharing and Analysis Organization. Information sharing, however, is core to the other dimensions of the CCSMM and having organizations within a community communicate on the way each is implementing the various parts of the CCSMM will help the entire community cooperatively progress in the maturity of individual and community programs.

The federal government has increasingly learned that national cybersecurity is not simply a matter of concern for the government. The majority of cyber infrastructures are not owned and/or operated by the federal government which has a limited ability to impact its security. The need for a public/private partnership is required to address security nationally. This is also true at a state and local level. It is not the responsibility of the state or a community to secure the private companies and organizations within its boundaries. At the same time, the government can serve as the catalyst, implementing things such as an ISAO, to encourage all members in its geographic boundaries to participate in security programs. Additionally, every community has emergency response plans for a number of different situations such as potential natural disasters or civil unrest. Similar plans should be developed for cybersecurity events within the boundaries of the state or community and an effective cybersecurity response will require the activity of both public and private organizations. A simple first step in this regard is the creation of a cybersecurity advisory board for mayors or city managers. This board can be called upon by city leadership in the event of a cyber event. In order to be more effective in a response to a cybersecurity event, periodic exercises should be conducted by both organizations and the community to ensure the plans that have been developed are sufficient, and are sufficiently understood, to address possible events. This can include both cyber-only exercises as well as incorporating cyber injects/events into other exercises such as a response to a natural disaster.

7. Integrating the CCSMM

An early step in both a state and a community, which can occur concurrently with the establishment of the ISAO, is to assess the overall maturity of the state or community's cybersecurity program. This will result in a classification in the CCSMM ranging from a level 1, Initial, to level 5, Vanguard as previously mentioned. Once the level is determined, the community (or state) ISAO can develop a plan to improve the cyber security program to reach the next level. It should be noted that not all communities will need to eventually be at a level 5. What level a community needs to reach should be determined based on the possible threats to the community. It should also be noted that one factor in the overall level obtained in a state or community is the level of preparedness of organizations within the community (or in the various communities for the state). It is not necessary for all organizations within a community to be at the same level. An assessment should be made of the major organizations that have an impact on the community (such as the utilities) to determine which are the most critical for the community and thus would have the most severe impact should the organization be attacked. Since private organizations can impact the community as a whole, it is important for community leadership to work with these organizations to ensure that they have implemented appropriate cyber security programs and are participating in the community ISAO. While the community can't force an organization to implement security measures, it will be important to establish relationships between all community organizations and have community leadership serve as the

champions for the community. An ISAO can help with this and the CCSMM can provide the roadmap for how the community and organizations within it can progress. A final point to make is how the CCSMM can help an organization determine what aspects of the NIST CSF can be implemented at the various levels of the CCSMM. At each level all five of the NIST CSF functions need to be addressed but it would be easy for an organization or for the community to become overwhelmed at the volume of things that can be done for each function if they are not broken down into which should be addressed first and what can be addressed at a later time.

8. Incorporating the NIST CSF

As was mentioned, all five functions need to be considered at each level of the CCSMM. The NIST CSF document contains considerable guidance on what can be done for each of these functions. Determining what needs to be done will occur as the community examines the goals at each level of the CCSMM. The ISAO will also become of tremendous benefit as the various organizations within the community attempt to implement the five functions as they establish, then advance, their cybersecurity programs. Comparing notes on how various aspects were incorporated within different organizations will help facilitate the adoption of the CSF throughout the community.

9. Summary and Way Ahead

There is no doubt that cybersecurity is becoming more of an issue for states and communities as the number and types of attacks that they experience are growing and becoming more sophisticated. Trying to "do it on your own" really is not an option for most communities as they do not have the budget or experience to try and establish their own programs. Documents such as the NIST CSF provide a lot of guidance on what a robust program should include but getting started using this document (and associated guidance) can be daunting for any community, not to mention smaller communities that don't even have a full-time cybersecurity administrator. At the same time, there are other programs and other guidance that can be combined into an overall security approach that will help states and communities, no matter what the size, to begin and to grow their programs.

The establishment of an ISAO will help to bring a community and state together as individuals and organizations within the community attempt to address cybersecurity for the community as a whole. It is not solely the responsibility of local and state government to begin security programs, it must be a public/private partnership to ensure that all critical functions within a community are addressed. The public/private partnership can also aid in the development of trusted relationships as the various cybersecurity personnel come together to advance their own security programs and to address security within the community. We have seen that the type of attack that occurs may be hard to detect should an organization or even a sector within a community attempt to address it on its own. Some attacks may only be initially detected by looking at activities across the community which can be done with the establishment of a community ISAO.

Finally, it is unreasonable to expect all communities in all states to immediately grasp the importance of cybersecurity to their community. In order to advance the concept of community and state ISAOs an overall organization needs to be established with the goal of helping communities and states to create their own ISAOs. (Some states are currently creating their own ISAOs and ISACs but these are generally designed to address only the traditional information sharing and analysis functions as seen in the current ISAC community.) Consequently, in August of 2018 the Geographically-Based Community ISAOs (GBC ISAOs) was established to assist communities in developing a basic template for how a community ISAO can be organized, how it can assist in the incorporation of the CCSMM, and how and at what point the various elements found in the NIST CSF can and should be implemented. The goal of the GBC ISAOs is to advance the state of the nation's cybersecurity posture by assisting states and communities in creating their own viable cybersecurity programs. This will not be completed overnight, but it is a tremendous first step in establishing the grass-roots level program that the nation needs.

10. References

[1] Tod Newcombe, "Small Towns Confront Big Cyber-Risks", *Government Technology* (online), http://www.govtech.com/security/GT-OctoberNovember-2017-Small-Towns-Confront-Big-Cyber-Risks.html, October/November 2017.

[2] Bill Clinton, “Critical Infrastructure Protection”, Presidential Decision Directive /NSC 63, May 22, 1998.

[3] Barack Obama, “Promoting Private Sector Cybersecurity Information Sharing”, Executive Order 13691, February 20, 2015.

[4] K. Harrison, J. Rutherford, G. White, “The Honey Community: Use of Combined Organizational Data for Community Protection”, HICSS-48, Kauai, HI, January 7, 2015

[5] G. White, “A Grassroots Cyber Security Program to Protect the Nation”, HICSS-45, Maui, HI, January 4-7, 2012.

[6] NIST, “Framework for Improving Critical Infrastructure Cybersecurity”, version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.0,416 2018.pdf

[7] Multi State ISAC, homepage
https://www.cisecurity.org/ms-isac/